

# PROGRAM PERFORMANCE CONTROLLER

**Patent number:** JP2002041170  
**Publication date:** 2002-02-08  
**Inventor:** KANAMARU TOMOKAZU; WAKE HIROYUKI; TOMINAGA NOBUTERU; HARUNA NAOSUKE  
**Applicant:** MATSUSHITA ELECTRIC IND CO LTD  
**Classification:**  
 - **International:** G06F1/00; G06F12/14  
 - **European:**  
**Application number:** JP20000227840 20000727  
**Priority number(s):**

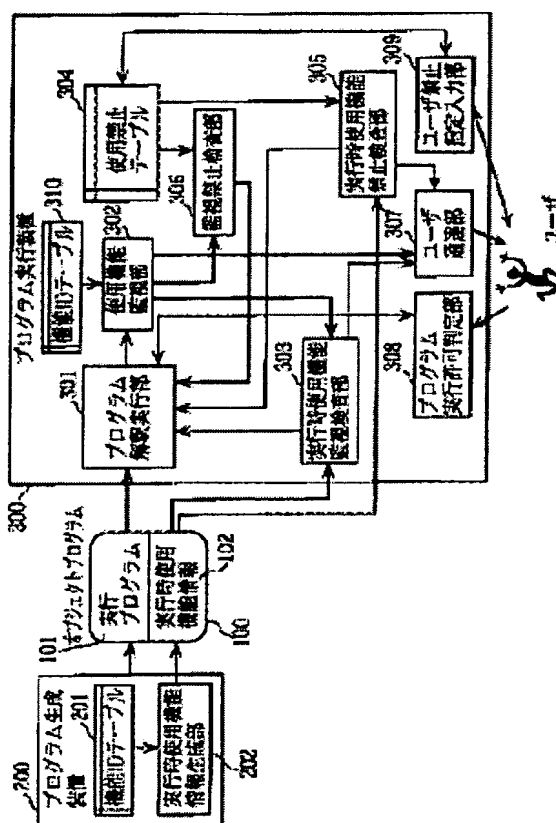
Also published as:

JP2002041170 (A)

## Abstract of JP2002041170

**PROBLEM TO BE SOLVED:** To provide a means for easily assuring security at the time of performing a downloaded program.

**SOLUTION:** A program performing device 300 mounted on a portable telephone set acquires a performance program 101 to which performance time the function information 102 declaring a function to be used is added from a communication passage, and allows a program interpretation performing part 301 to successively execute the performance program. At the time of performing the performance program 101, the program performing device 300 stops the performance when the use of any function included in a user inhibition table 304 indicating any function whose use is inhibited is declared by the performance time use function information 102. Also, the program performing device 300 monitors an instruction to be performed the next during the performance of the performing program 101, and stops the performance when the use of any function used by the instruction is not declared by the performance time use function information 102.



Data supplied from the esp@cenet database - Worldwide

BEST AVAILABLE COPY

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-41170

(P 2002-41170A)

(43) 公開日 平成14年2月8日(2002.2.8)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	ターマコード <sup>*</sup>	(参考)
G06F 1/00		G06F 12/14	310	Z 5B017
12/14	310	9/06	660	J 5B076

審査請求 未請求 請求項の数17 O L (全16頁)

(21)出願番号 特願2000-227840(P2000-227840)

(22) 出願日 平成12年7月27日(2000.7.27)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 金丸 智一

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 發明者 和氣 裕之

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗 (外1名)

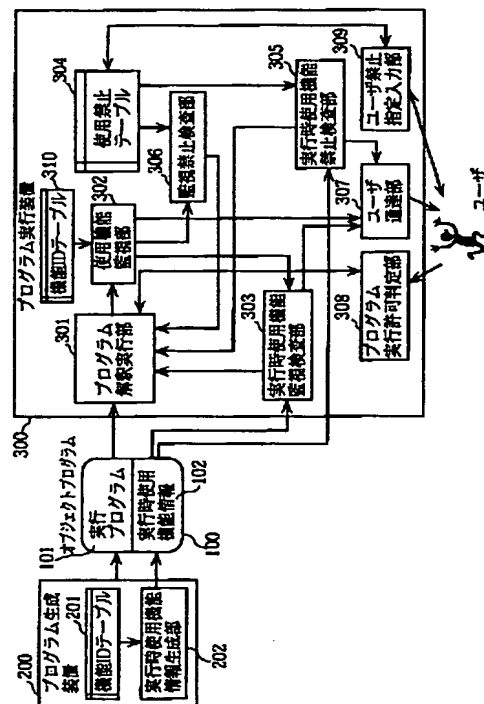
[最終頁に続く](#)

(54) 【発明の名称】 プログラム実行制御装置

(57) 【要約】

【課題】 ダウンロードしたプログラムの実行に際してのセキュリティ確保を簡易に行う手段を提供する。

【解決手段】 携帯電話機に搭載されたプログラム実行装置３００は、使用する機能を宣言した実行時使用機能情報１０２が付加された実行プログラム１０１を通信路より取得して、プログラム解釈実行部３０１によって逐次実行する。実行プログラム１０１の実行に際して、プログラム実行装置３００は、使用を禁止する機能を示す使用禁止テーブル３０４に含まれる機能が実行時使用機能情報１０２において使用宣言されていると実行を停止する。また実行プログラム１０１の実行中に次に実行する命令を監視することにより、その命令により利用される機能が実行時使用機能情報１０２で使用宣言されていないものであれば実行を停止する。



BEST AVAILABLE COPY

## 【特許請求の範囲】

【請求項 1】 機器に搭載されており、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたプログラムを取得して、実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、前記使用機能情報に基づく判断を行い、判断結果がプログラムの実行が不適当であることを表す所定の場合に、前記実行手段によるプログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項 2】 前記プログラムは複数の命令を含み、前記実行手段は前記プログラム中の命令を実行するものであり、前記停止手段は、実行中のプログラムにおける次に実行対象となる命令を監視し、前記命令が前記機能群のうち前記使用機能情報において使用する機能として示されていない機能を使用する命令であった場合に前記実行手段による前記プログラムの実行を停止させることを特徴とする請求項 1 記載のプログラム実行制御装置。

【請求項 3】 前記使用機能情報は暗号化されており、前記停止手段は前記使用機能情報を復号して参照することを特徴とする請求項 2 記載のプログラム実行制御装置。

【請求項 4】 前記プログラム実行制御装置は、使用を禁止する機能を示す禁止機能情報を記憶する禁止機能記憶手段を備え、前記停止手段は、前記禁止機能情報に示されている使用を禁止する機能が前記使用機能情報に使用する機能として示されている場合には前記実行手段によるプログラムの実行を停止させることを特徴とする請求項 1 記載のプログラム実行制御装置。

【請求項 5】 前記禁止機能情報が示す使用を禁止する機能には、少なくとも無線通信の機能が含まれることを特徴とする請求項 4 記載のプログラム実行制御装置。

【請求項 6】 前記禁止機能情報が示す使用を禁止する機能には、少なくとも出力デバイスからのデータ出力の機能が含まれることを特徴とする請求項 4 記載のプログラム実行制御装置。

【請求項 7】 前記禁止機能情報が示す使用を禁止する機能には、少なくとも入力デバイスからのデータ取得の機能が含まれることを特徴とする請求項 4 記載のプログラム実行制御装置。

【請求項 8】 前記プログラム実行制御装置はさらに、ユーザの操作を受け付けて前記操作に応じて前記禁止機能情報を更新する禁止機能変更手段を備えることを特徴とする請求項 4～7 のいずれか 1 項に記載のプログラム実行制御装置。

【請求項 9】 個人情報領域を有するメモリを備える携

帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域からのデータ読出を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

10 【請求項 10】 個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域へのデータ書込を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

20 【請求項 11】 携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末の外部と通信する機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項 12】 前記機能処理ルーチンは前記携帯情報端末の外部へのデータ送信を行う機能処理ルーチンであることを特徴とする請求項 11 記載のプログラム実行制御装置。

【請求項 13】 携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える出力デバイスからのデータ出力を行う機能処理ルーチンを呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

40 【請求項 14】 携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、

通信路からプログラムを取得する取得手段と、  
取得したプログラムを実行する実行手段と、  
実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える入力デバイスからのデータ取得を行う機能処理ルーチンと呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とするプログラム実行制御装置。

【請求項 15】 前記プログラム実行制御装置はさらに、  
前記停止手段によって前記プログラムの実行が停止した場合に、停止した旨をユーザに通知する通知手段を備えることを特徴とする請求項 1～14 のいずれか 1 項に記載のプログラム実行制御装置。

【請求項 16】 前記プログラム実行制御装置はさらに、  
前記停止手段によって前記プログラムの実行が停止した場合に、ユーザによる入力を受け付けて前記入力に応じて停止を解除する停止解除手段を備えることを特徴とする請求項 1～15 のいずれか 1 項に記載のプログラム実行制御装置。

【請求項 17】 プログラム実行機能を有する機器に、  
前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたオブジェクトプログラムを取得して実行するプログラム実行制御処理を、行わせる制御プログラムを記録した記録媒体であって、  
前記プログラム実行制御処理は、  
通信路からオブジェクトプログラムを取得する取得ステップと、  
取得したオブジェクトプログラムを実行する実行ステップと、  
前記使用機能情報に基づく判断を行い、判断結果がオブジェクトプログラムの実行が不適当であることを表す所定の場合に、オブジェクトプログラムの実行を停止させる停止ステップとを備えることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、不正なプログラムの実行による被害を防ぐ技術に関し、特に携帯情報端末用のアプリケーションプログラムをダウンロードして携帯情報端末上で実行する場合におけるセキュリティ確保のための技術に関する。

【0002】

【従来の技術】近年、通信技術、ソフトウェア技術等の進展を背景として、家電機器や携帯情報端末（以下、「家電機器等」という。）の機能の拡張等を実現するために、CPU が組み込まれた家電機器等に対するプログラムの配信サービスについての研究開発の要請が高まっ

ている。

【0003】家電機器等がプログラムの配信サービスに対応する機能を備えれば、家電機器等は外部のネットワーク上のサーバに用意されたアプリケーションプログラムをダウンロードすることができ、必要な時にそのアプリケーションプログラムを実行することができるようになる。従って、家電機器等のユーザは、家電機器等に最初から作り込まれている機能のみならず、後からダウンロードにより追加された種々の機能を利用することができ、例えばユーザは自己の望む機能を実現するアプリケーションプログラムを任意に選択しダウンロードして利用すること等が可能になる。

【0004】例えば、携帯情報端末への配信サービスの対象としては通話及び通信機能に密接に関連した機能のアプリケーションプログラムやアドレス帳、ゲーム等の様々なアプリケーションプログラムが考えられる。配信サービスの対象となるアプリケーションプログラムは、基本的に、家電機器等を製造しているメーカーやその関連企業等によって作成される。また、家電機器等のメーカー等から特定機器用のアプリケーションプログラムの開発環境となるツール類等の配布を受けた、一般のプログラム開発者や企業によって作成される場合も考えられる。

【0005】こうしてメーカーその他の者により作成されたアプリケーションプログラムを家電機器等の側でダウンロードして利用する場合を想定すると、家電機器等にはセキュリティ確保のための機能が備えられている必要がある。なぜなら、メーカー等により正当なものとして作成されたアプリケーションプログラムが悪意ある者によって、望ましくない動作を行うように不正に改変されている場合があり、また、一般のプログラム開発者等により、望ましくない動作を行うアプリケーションプログラムが提供されている場合もないとはいえないからである。

【0006】アプリケーションプログラムによる望ましくない動作としては、機器内のデータ記憶領域内のデータを勝手に更新するような動作があり、携帯電話機等の携帯情報端末においては内部に記憶されている電話番号、メールアドレスその他のプライバシーに関わる情報（以下、「個人情報」という。）の読み出しや外部への発呼等も、ユーザの意思に沿わない場合は望ましくない動作といえる。

【0007】ところで、従来パーソナルコンピュータ等の分野ではインターネットからダウンロードしたアプリケーションプログラムの実行時におけるセキュリティ確保を実現する仕組みとして、Java（登録商標）仮想マシンのコードベリファイアという機構がある。コードベリファイアは、アプリケーションプログラムである Java クラスファイルを解釈実行する前に、そのフォーマットや命令列を検査し、静的制約や構造体制約に従っ

て、ダウンロードされたJavaクラスファイルが実行中に危険な動作を行わないことを保証する。このコードベリファイアについては、「The Java Virtual Machine Specification」(Tim Lindholm、Frank Yellin著、Addison-Wesley、1997年)に詳しく記述されている。

#### 【0008】

【発明が解決しようとする課題】しかしながら、このコードベリファイアによるアプリケーションプログラムの正当性の検査は、複雑な処理であるため多大な処理ステップを要する。従って、Javaクラスファイルを実行するためにはクロック周波数が最低でも100MHz以上の高性能のCPUや2MByte~4MByteの大きなメモリの空き容量等、高価なコンピュータ資源が必要となる。これは現在においては大部分の家電機器等にとって過大な資源量であるため、コードベリファイアを備えることは、家電機器等にとって現実的なセキュリティ確保の手段とはならない。

【0009】そこで、本発明は、家電機器等に向けて配信サービスの対象とされたアプリケーションプログラムを家電機器等がダウンロードして実行する際のセキュリティ確保を図る必要があることに鑑みてなされたものであり、家電機器等、特に携帯情報端末に適用し得るように比較的簡易な方法により、アプリケーションプログラムをダウンロードして実行する際のセキュリティ確保を実現するプログラム実行制御装置を提供することを目的とする。

#### 【0010】

【課題を解決するための手段】上記課題を解決するために、本発明に係るプログラム実行制御装置は、機器に搭載されており、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたプログラムを取得して、実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、前記使用機能情報に基づく判断を行い、判断結果がプログラムの実行が不適当であることを表す所定の場合に、前記実行手段によるプログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0011】上記構成により、予めプログラムに、そのプログラムが使用する機能を示す使用機能情報が付加されているので、この使用機能情報を利用することにより比較的簡易な方法でセキュリティを確保することが可能になる。即ち、使用機能情報と実際のプログラムの動作とを比べることによりそのプログラムが改竄されていることを検出することや、使用機能情報を参照することにより、使用を禁止すべき機能をそのプログラムが使用するかどうかを検出することが簡易な構成で実現できるようになる。

#### 【0012】

【発明の実施の形態】以下、本発明の実施の形態であるプログラム実行装置について説明する。

<構成>図1は、本発明の実施の形態に係るプログラム実行装置300等の構成図である。

【0013】同図には、携帯電話機に備えられるプログラム実行装置300の他に、プログラム実行装置300において実行されるオブジェクトプログラム100と、オブジェクトプログラム100を生成するプログラム生成装置200とをも示している。

<プログラム生成装置>プログラム生成装置200は、実行時使用機能情報を付加したオブジェクトプログラムを生成する装置であり、コンピュータ上で動作するコンパイラ及びリンカである。このオブジェクトプログラムはプログラム実行装置300上で動作する実行形式のプログラムを意味するものであり、アプリケーションプログラムである。なお、実行時使用機能情報については後述する。

【0014】プログラム生成装置200は、従来のコンパイラ及びリンカと同等の機能に加えて実行時使用機能情報を生成する機能を有し、実行時使用機能情報を生成する機能を実現するために機能IDテーブル201と実行時使用機能情報生成部202とを備える。図3は、機能IDテーブルのデータ構造及び内容例を示す図である。

【0015】機能IDテーブルは機能ID401とライブラリ番号402との組の集合からなるテーブルである。同図に示した内容例では、0x0001という機能IDは6というライブラリ番号が対応付けられている。ここで、機能ID401はプログラム実行装置300上で動作するオブジェクトプログラムが利用する各機能の識別子である。なお、運用上の前提としてプログラム実行装置300上で動作するオブジェクトプログラムが利用できる各機能は予め分類整理され、それぞれに識別子が定められていることとする。

【0016】また、ライブラリ番号402は、オブジェクトプログラム内で呼び出しが可能なライブラリプログラムの番号である。即ち、オブジェクトプログラムの動作環境であるプログラム実行装置300上に用意されたライブラリプログラムの番号である。なお、ライブラリ呼び出しにより使用し得る機能は、例えば無線インタフェースへのデータ出力機能、ディスプレイへのデータ出力機能、音声出力回路へのデータ出力機能、無線インタフェースからのデータ入力機能、ボタンからのデータ入力機能等がある。図3の内容例では括弧内に機能IDの意味する機能を便宜上付記している。

【0017】実行時使用機能情報生成部202は、プログラム生成装置200が従来のコンパイラ及びリンカと同等の機能によりオブジェクトプログラムを生成した後

いるライブラリプログラムを検索して機能IDテーブル201に照らして機能IDを得ることにより、オブジェクトプログラムが使用する機能を示す実行時使用機能情報を生成し、そのオブジェクトプログラムに付加する。

【0018】図4は、オブジェクトプログラムに付加される実行時使用機能情報のデータ構造及び内容例を示す図である。実行時使用機能情報は、オブジェクトプログラムがライブラリ呼び出しによって使用し得る全ての機能について、機能ID毎に実際にその情報の付加先となるオブジェクトプログラムが使用しているか否かを示すフラグ502を対応付けた情報である。フラグ502は、0x00が使用しない旨を示し、0x01が使用する旨を示す。

【0019】同図の内容例は、例えば機能IDが0x0001の機能は使用されず、機能IDが0x0002の機能は使用されることを示している。このようなプログラム生成装置200によって生成されたオブジェクトプログラム100は図1に示すように、実行プログラム101と実行時使用機能情報102とから構成されるものとなる。ここで、実行プログラム101は、通常のオブジェクトプログラム自体であり、プログラム実行装置300上で解釈実行されるものである。

【0020】オブジェクトプログラム100は、例えばJavaクラスファイルであり、実行時使用機能情報102は、Javaクラスファイル中にアトリビュート情報として置かれる。なお、Javaクラスファイルはアトリビュート情報を付加することができるものである。またアトリビュート情報は識別番号を設定できるものであり、特定のJava仮想マシンとの間での取決めに従ってその内容を定めることができる。つまり、特定の識別番号のアトリビュート情報を解釈できるようにJava仮想マシンを構築しておくことが可能になっている。また、Java仮想マシンの仕様では、その特定の識別番号のアトリビュート情報を解釈できないJava仮想マシンはそのアトリビュート情報を読み飛ばすこととされている。

【0021】ここでは、実行時使用機能情報102は、プログラム実行装置300がオブジェクトプログラム100を取得して実行する際にメモリにロードした時点でプログラム実行装置300によって参照され得るものであることとする。

＜プログラム実行装置＞プログラム実行装置300は、携帯電話機内に備えられ、オブジェクトプログラム100を取得して実行する装置であり、オペレーティングシステム及びJava仮想マシンを含むものである。

【0022】プログラム実行装置300は、図1に示すようにプログラム解釈実行部301、使用機能監視部302、実行時使用機能監視検査部303、使用禁止テーブル304、実行時使用機能禁止検査部305、監視禁止検査部306、ユーザ通達部307、プログラム実行

許可判定部308、ユーザ禁止指定入力部309及び機能IDテーブル310を有する。これらプログラム解釈実行部301その他各部は、基本的に携帯電話機のメモリに備えられた制御プログラムがCPUにより実行されることによりその機能を発揮する。

【0023】ここで、プログラム解釈実行部301は、実行プログラム101を解釈実行するものであり、基本的には従来のJava仮想マシンと同様にJavaクラスファイルを逐次解釈実行するいわゆるインタプリタである。但し、プログラム解釈実行部301は通常のインタプリタとしての機能に加えて、実行プログラム101の解釈実行中に、実行時使用機能監視検査部303、実行時使用機能禁止検査部305又は監視禁止検査部306の通知を受けることにより解釈実行を停止できる機能を有している。

【0024】使用機能監視部302は、プログラム解釈実行部301が実行プログラム101を解釈実行しているときに、次に実行されようとしているJavaバイトコード（以下、「命令」ともいう。）を監視して、予め定められている機能のうちいずれかが使用されようとした場合に、その使用されようとした機能についての機能IDを出力する。即ち、使用機能監視部302は、実行プログラム101を逐次解釈しているプログラム解釈実行部301から、次にプログラムカウンタが指す位置の命令、つまり次に実行しようとしている命令を通知され、機能IDテーブル310を参照して後述する監視処理を行うことにより、その命令に対応する機能IDを得て、機能IDを出力する。

【0025】実行時使用機能監視検査部303は、使用機能監視部302から出力された機能IDと実行時使用機能情報102とを入力とし、実行時使用機能情報102において使用しない旨のフラグに対応付けられている機能IDが使用機能監視部302から出力された場合には、実行プログラム101の解釈実行を停止するようにプログラム解釈実行部301に伝える。

【0026】使用禁止テーブル304は、プログラム実行装置300上で動作するアプリケーションプログラムに使用され得る全ての機能それぞれについて、ダウンロードしたオブジェクトプログラム100の実行プログラム101に対してその機能を使用することを許可しているか禁止しているかを示す情報を記録したテーブルである。

【0027】図5は、使用禁止テーブル304のデータ構造及び内容例を示す図である。同図に示すように使用禁止テーブルは機能ID601とその機能IDで示される機能の使用が許可されているか禁止されているかを示すフラグ602との組の集合からなるテーブルである。機能ID601は、アプリケーションプログラムに使用され得る機能を区分して、区分された各機能に一意となるように識別子を割り当てたものであり、その各機能に

は、アプリケーションプログラムから呼び出されるライブラリに対応した機能が含まれ、さらにロード命令やストア命令に対応する機能が含まれる。つまり、使用禁止テーブルには、機能IDテーブル又は実行時使用機能情報に含まれる機能IDを全て包含した上にロード命令やストア命令に対応する機能IDが含まれる。

【0028】フラグ602は、0x00が使用を禁止する旨を示し、0x01が使用を許可する旨を示す。同図に示す内容例では、例えば、ロード命令に対応するものとして、個人情報領域からのデータ読出を意味する0x0101という機能IDの機能と、システム領域からのデータ読出を意味する0x0102という機能IDの機能と、ストア命令に対応するものとして、個人情報領域へのデータ書込を意味する0x0201という機能IDの機能と、システム領域へのデータ書込を意味する0x0202という機能IDの機能とは、使用が禁止されていることを示している。なお、個人情報領域及びシステム領域については後に説明する。

【0029】また、実行時使用機能禁止検査部305は、実行時使用機能情報102と使用禁止テーブル304とを参照して、これらを比較することにより、実行時使用機能情報102において使用する旨のフラグに対応付けられている機能IDと同一の機能IDが使用禁止テーブル304においては使用を禁止する旨のフラグに対応付けられている場合には、実行プログラム101の解釈実行を停止するようにプログラム解釈実行部301に伝える。

【0030】監視禁止検査部306は、使用機能監視部302から出力された機能IDと使用禁止テーブル304とを入力とし、使用禁止テーブルにおいて使用を禁止する旨のフラグに対応付けられている機能IDが使用機能監視部302から出力された場合には、実行プログラム101の解釈実行を停止するようにプログラム解釈実行部301に伝える。

【0031】ユーザ通達部307は、プログラム解釈実行部301による実行プログラム101の解釈実行が停止した旨を携帯電話機のディスプレイに表示するよう制御して、プログラムの実行停止をユーザに通達するものである。プログラム実行許可判定部308は、ユーザ通達部307とともに解釈実行の停止時におけるユーザインタフェースを構成するものであり、実行プログラム101の解釈実行の停止の旨をユーザ通達部307がディスプレイに表示するよう制御した場合に、実行プログラム101の停止を解除するか又は実行プログラム101の実行を終了するかユーザによる指定を携帯電話機の各種ボタン等を通じて受け付け、その指定に応じてプログラム解釈実行部301に対して停止の解除又は終了の指示を伝える。

【0032】ユーザ禁止指定入力部309は、使用禁止テーブル304の内容の変更についての入力を携帯電話

機の各種ボタン等を通じてユーザから受け付け、その入力に応じて使用禁止テーブル304を更新する。ユーザ禁止指定入力部309が存在することによって、ユーザはダウンロードしたアプリケーションプログラムにより特定の機能が使用されることを許可するか禁止するかを指定することができる。

【0033】また、機能IDテーブル310は、機能IDテーブル201と同一内容のテーブルであり、図3に示す構造を有するテーブルである。なお、プログラム実行装置300は、無線基地局を介して通信によりアプリケーションプログラムを取得、即ちダウンロードして携帯電話機に備えられたメモリに格納する機能を有する。

【0034】図2は、プログラム実行装置300を備える携帯電話機320とダウンロード対象のオブジェクトプログラムとの関係を示す図である。公衆網に接続されたコンピュータであるプログラム格納サーバ250には携帯電話機にダウンロードされることを目的としてプログラム生成装置200を備えるプログラム生成系から提供されたオブジェクトプログラム100が格納されている。プログラム実行装置300を備える携帯電話機320は、無線基地局260と無線通信することにより無線基地局260を介してプログラム格納サーバ250に格納されているオブジェクトプログラム100をダウンロードすることができる。

【0035】＜メモリ構造＞ここで、プログラム実行装置300が実行するアプリケーションプログラムがアクセスし得るメモリについて説明する。メモリは、個人情報を記録するための個人情報領域と、オペレーティングシステムやインタプリタ機能の実行に必要な情報を記録するためのシステム領域と、その他の領域とに分けられる。

【0036】図6は、メモリ内の領域の分類を示した図である。同図に示すようにメモリは0x0000番地から0x3FFF番地までがシステム領域であり、0x4000番地から0x7FFF番地までが個人情報領域であり、0x8000番地から0xFFFF番地までがシステム領域でも個人情報領域でもないその他の領域である。

【0037】つまり、携帯電話機に最初から内蔵されたアプリケーションプログラムによって、個人情報は個人情報領域に記録されるようになっており、またプログラム実行装置300はシステム領域にアクセスして処理の実行に必要なデータの記録及び読み出しを行うものである。図7は、個人情報の内容の具体例を示す図である。同図に示すように、個人情報は、人物名や電話番号等の個人のプライバシーに関わる情報を含んでいる。従って、この個人情報領域に格納されている個人情報は不正なアクセスから特に保護されるべきである。

＜動作＞以下、上述の構成を備えるプログラム実行装置300の動作について説明する。

【0038】＜解釈実行動作＞図8は、プログラム実行装置300がダウンロードしたオブジェクトプログラムを解釈実行する際における処理手順を示すフローチャートである。プログラム実行装置300は、無線基地局との通信によりオブジェクトプログラム100をダウンロードし、メモリに格納した後、解釈実行を始める。

【0039】プログラム解釈実行部301が実行プログラム101の解釈実行を行うに際して、まず実行時使用機能禁止検査部305は、Javaクラスファイルの特定の識別番号で識別されるアトリビュート情報を参照することにより実行時使用機能情報102にアクセスし、実行時使用機能情報102と使用禁止テーブル304とを比較し(ステップS101)、実行時使用機能情報102において使用する旨のフラグと対応付けられている機能IDのうちいずれかが、使用禁止テーブルにおいて使用が禁止されている旨のフラグと対応付けられている機能IDと一致するか否かを判定する(ステップS102)。

【0040】ステップS102において一致すると判定した場合には、実行時使用機能禁止検査部305はプログラム解釈実行部301及びユーザ通達部307に停止を通知しプログラム実行装置300は解釈実行停止処理を行い(ステップS103)、一致しないと判定した場合にはステップS103をスキップし、続いて監視処理を行う(ステップS104)。なお、解釈実行停止処理については後に説明する。

【0041】ここで、監視処理を説明する。図9は、使用機能監視部302による監視処理を示すフローチャートである。プログラム解釈実行部301はプログラムカウンタを参照して次に実行する命令を得て使用機能監視部302に伝える(ステップS201)。使用機能監視部302は、その命令がaload等のデータ読出命令であるか否かを判定し(ステップS202)、データ読出命令であれば、その命令のオペランドに基づいて、メモリ内の読出対象となる位置である読出アドレスを取得する(ステップS203)。読出アドレスがレジスタ等によって指定されている場合であっても、ステップS203の実行の際におけるそのレジスタ等の内容値を参照することによって実際の読出アドレスを取得する。

【0042】読出アドレスを取得した後、その読出アドレスはシステム領域内を指すものであるか否かを判定し(ステップS204)、システム領域内を指すものであれば0x0102という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS205)。ステップS204においてシステム領域内を指すものでなければ、読出アドレスは個人情報領域内を指すものであるか否かを判定し(ステップS206)、個人情報領域内を指すものであれば0x0101という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視

処理を終了する(ステップS207)。

【0043】ステップS206において個人情報領域内を指すものでなければ、0x0000という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS208)。得た命令がデータ読出命令でない場合には(ステップS202)、使用機能監視部302はその命令がastore等のデータ書込命令であるか否かを判定し(ステップS209)、データ書込命令であれば、その命令のオペランドに基づいて、メモリ内の書込対象となる位置である書込アドレスを取得する(ステップS210)。書込アドレスがレジスタ等によって指定されている場合であっても、ステップS210の実行の際におけるそのレジスタ等の内容値を参照することによって実際の書込アドレスを取得する。

【0044】書込アドレスを取得した後、その書込アドレスはシステム領域内を指すものであるか否かを判定し(ステップS211)、システム領域内を指すものであれば0x0202という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS212)。ステップS211においてシステム領域内を指すものでなければ、書込アドレスは個人情報領域内を指すものであるか否かを判定し(ステップS213)、個人情報領域内を指すものであれば0x0201という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS214)。

【0045】ステップS213において個人情報領域内を指すものでなければ、0x0000という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS215)。得た命令がデータ書込命令でない場合には(ステップS209)、使用機能監視部302はその命令がinvokevirtual等のライブラリ呼出命令であるか否かを判定し(ステップS216)、ライブラリ呼出命令であれば、その命令のオペランドからライブラリ番号を得て、そのライブラリ番号に対応する機能IDを機能IDテーブル310を参照することにより取得して、その機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS217)。

【0046】また、ステップS216においてライブラリ呼出命令でなければ、使用機能監視部302は、0x0000という機能IDを実行時使用機能監視検査部303及び監視禁止検査部306に伝えて監視処理を終了する(ステップS218)。なお、使用機能監視部302から出力される機能IDは、ライブラリ呼出命令に対応する機能IDかそれ以外の命令に対応する機能IDかが識別できるようになっており、ここでは、機能IDのうち上位8ビットが0x00であるものがライブラリ呼



出命令に対応するものであることとしている。

【0047】以下、図8に即した説明に戻る。上述した監視処理（ステップS104）の後、実行時使用機能監視検査部303は監視処理の結果として使用機能監視部302から出力された機能IDと、実行時使用機能情報102との比較検査を行い（ステップS105）、実行プログラム101中の次に実行される命令によって使用される機能の機能ID即ち監視処理の結果として出力された機能IDと同一の機能IDが実行時使用機能情報102において使用しない旨のフラグと対応付けられているか否かを判定する（ステップS106）。ステップS106は、実行時使用機能情報102によって使用しないと宣言している機能を、実際の実行に際しては使用しようとしていたか否かを判定するという意味を持つ。

【0048】ステップS106において監視処理の結果として出力された機能IDが実行時使用機能情報102において使用しない旨のフラグと対応付けられている機能IDであった場合に限り、実行時使用機能監視検査部303はプログラム解釈実行部301及びユーザ通達部307に停止を通知しプログラム実行装置300は解釈実行停止処理を行い（ステップS107）、その他の場合にはステップS107をスキップし、その後に監視処理の結果として出力された機能IDと使用禁止テーブルとの比較検査を監視禁止検査部306が行う（ステップS108）。

【0049】ステップS108においては監視禁止検査部306は監視処理の結果として出力された機能IDと同一の機能IDが使用禁止テーブルにおいて使用を禁止する旨のフラグと対応付けられているか否かを判定する（ステップS109）。この判定の結果、監視処理の結果として出力された機能IDが使用禁止テーブルにおいて使用を禁止する旨のフラグと対応付けられている機能IDであった場合に限り監視禁止検査部306はプログラム解釈実行部301及びユーザ通達部307に停止を通知し解釈実行停止処理を行い（ステップS110）、その他の場合にはステップS110をスキップする。

【0050】続いて、監視処理の対象となった命令即ち次に実行されるべき命令をプログラム解釈実行部301が解釈実行する（ステップS111）。プログラム解釈実行部301による実行プログラム101の全ての処理の解釈実行が終了するまでステップS104からS111の処理が繰り返され、全ての処理の解釈実行が終了するとプログラム実行装置の動作も終了する（ステップS112）。

【0051】以下、解釈実行停止処理について説明する。図10は、解釈実行停止処理を示すフローチャートである。停止の通知を受けたプログラム解釈実行部301は実行プログラムの解釈実行を停止するように内部の変数等による制御状態を設定し（ステップS301）、ユーザ通達部307は解釈実行が停止されたことをユー

ザに通達する（ステップS302）。

【0052】このステップS302におけるユーザ通達部307の制御によりディスプレイに表示される画面は、例えば図11に示すものとなる。この画面はファイル名がmaze.cjである実行プログラム101の実行が停止された旨を示すとともにユーザに対して実行の継続を指示する場合に用いるボタンを知らせるものである。

【0053】ユーザ通達部307によるユーザへの停止の通達の後にはプログラム実行許可判定部308はユーザの入力を受け付け解釈し（ステップS303）、実行プログラム101の解釈実行を継続する旨の指示の入力であるか否かを判断する（ステップS304）。ステップS304において解釈実行の継続の指示と判断した場合にはプログラム実行許可判定部308はプログラム解釈実行部301に解釈実行の停止の解除を指示し、これを受けてプログラム解釈実行部301は解釈実行の停止を解除するように制御状態を設定する（ステップS305）。このステップS305により実行プログラム101は引き続き解釈実行されるものとなる。

【0054】またステップS304において解釈実行の継続の指示でないと判断した場合にはプログラム実行許可判定部308はプログラム解釈実行部301に解釈実行の終了を指示し、これを受けてプログラム解釈実行部301は解釈実行を終了するように制御状態を設定する。（ステップS306）。このステップS306により実行プログラム101は以後解釈実行されることはなくなり、プログラム実行装置300の動作は終了する。

【0055】＜使用禁止テーブル更新動作＞プログラム実行装置300は、プログラムの解釈実行中以外の時において使用禁止テーブルの更新を行う機能を有する。この機能は、ユーザにより例えば携帯電話機の特定のボタンが押下された場合等の所定操作に対応して実行されるものであり、所定操作が行われるとユーザ禁止指定入力部309は携帯電話機のディスプレイに図12に示すような使用禁止機能選択画面を表示するよう制御して、ユーザによる使用禁止機能の指定に関する入力を受け付ける。

【0056】ユーザ禁止指定入力部309は、図12に示すように機能項目等を表示し、ユーザの特定のボタン操作に応じて機能項目の表示をスクロールさせ、また「1」又は「0」のボタン入力を受け付けると強調表示されている機能項目で表しているところの機能の使用を許可又は禁止とするように使用禁止テーブル304を更新する。

【0057】これにより、使用を禁止する機能をユーザが定めることができるようになる。例えば個人情報を読み出されても構わないと考えるユーザであれば、個人情報領域からのデータ読出の機能の使用を許可するように使用禁止テーブル304を変更することが可能になる。

<補足>以上、本発明に係るプログラム実行装置について実施の形態を用いて説明したが、本発明は実施の形態に示したものに限られることはない。即ち、

(1) 本実施の形態では、個人情報格納されるメモリ内の領域等はそのアドレスが固定的に定められているものとしたが、特定サイズのデータ毎にフラグを付加することとし、そのフラグにより個人情報であるかその他の情報であるかを識別できるようにしておくこととすれば、個人情報はメモリ空間内の任意のアドレスに分散して格納することも可能となる。つまり固定的でない特定サイズの個人情報領域が複数存在することとしてもよい。

【0058】図13は、メモリ内に個人情報であるデータと個人情報以外であるデータがフラグによって識別可能となるように格納されている例を示す図である。同図ではフラグは0か1の値を取り、フラグが1であれば個人情報であることを示している。このような場合には、監視処理における読出アドレス又は書込アドレスが個人情報領域内か否かの判断(ステップS206、S213)は、そのアドレスが指すデータに付加されたフラグが0か1かに基づいて行うこととする必要がある。なお、個人情報とシステムデータとその他のデータとを識別するようなフラグを特定サイズのデータ毎に付加することとすれば、同様の方法によりシステム領域内か否かの判断(ステップS204、S211)をも行うこととしてもよい。

(2) 本実施の形態において使用禁止テーブル304や実行時使用機能情報102等において示した機能の区分は単なる一例であり、他の区分であってもよい。また、機能IDテーブルはライブラリ呼出命令に対応する機能を列挙したテーブルとなっており、実行時使用機能情報102にはライブラリ呼出命令により実行され得る全ての機能について、使用するかしないかのフラグを対応付けた情報であるとしたが、ライブラリ呼出命令でない他の特定の命令により実行される機能についての情報を盛り込むこととしてもよい。但し、機能IDテーブル及び実行時使用機能情報に機能IDが含まれる機能は、その機能の使用の有無の確認がプログラムの実行前において簡易に行えるものとするのが望ましい。

【0059】なお、通常、プログラム実行装置が搭載された機器側に用意されたライブラリをオブジェクトプログラムが呼び出すことにより使用できる機能は、その機器の特定の資源を利用する機能であるため、機能IDテーブルはライブラリ毎に対応する機能を列挙したテーブルであることとすると、オブジェクトプログラムが危険動作を行うことを回避するというセキュリティ確保の目的を達成するためには適したものとなるといえる。

(3) 本実施の形態では、使用禁止テーブル(図5参照)により無線インタフェースへのデータ出力や無線インタフェースからのデータ入力を禁止する例を示した

が、これらを必ずしも禁止しなければならないことはなく、また他の回路へのデータ入出力を禁止することとしてもよいし、その他のライブラリ呼出によって実現される機能を禁止してもよい。また、無線インタフェースからのデータ入力及び無線インタフェースへのデータ出力の機能を禁止する代わりに外部への発呼機能、即ち電話をかける機能を禁止することとしてもよい。

【0060】なお、無線インタフェースを通じてのデータ入出力を禁止することは、ユーザが知らない内に外部と通信することを防ぐ意味において実用上有用である。また、例えばボタン、スイッチ、ダイヤル、マウス、トラックボール、ジョイスティック、キーボード、マイク、カメラ、センサ等の広い意味での入力デバイスからのデータ取得を禁止することや、ディスプレイ、LED、ランプ、スピーカー、パイプレータ等の広い意味での出力デバイスへのデータ出力を禁止することは、盗聴等の不正な情報取得の防止や、迷惑な出力の防止の面において有用な場合がある。

【0061】また、本実施の形態では、使用禁止テーブルにより個人情報領域からのデータ読出、システム領域からのデータ読出、個人情報領域へのデータ書込及びシステム領域へのデータ書込を禁止する例を示したが、これらを必ずしも禁止しなければならないことはなく、またその他の特定の命令の実行を禁止するようにしてもよい。なお、個人情報へのアクセスを禁止することは、プライバシー保護等の面から実用上有用である。

(4) 本実施の形態において図10のステップS303で示したユーザの入力は、ボタンに限らず、他の入力デバイスを介してなされることとしてもよい。また、ステップS303においては、予め定められた取決めに従って、ユーザが操作をなさなかったことを特定の指定を入力したものと解釈することにしてもよい。例えば、実行プログラムが停止した旨がディスプレイに表示されてから30秒間何も入力しなければ、プログラム実行許可判定部308はその実行プログラムの解釈実行の継続を行わないという指定がユーザによりなされたと解釈することとしてもよい。

(5) 本実施の形態において図2に示したオブジェクトプログラム100を携帯電話機がダウンロードする際には、そのオブジェクトプログラム100の配信側であるプログラム格納サーバ250の正当性を確認するために、相互認証等を行うこととしてもよい。

【0062】また、本実施の形態では、プログラム実行装置300は携帯電話機に備えられるものとしたが、これに限定されるものではなく、他の家電機器や携帯情報端末に適用されるものであることとしてもよい。また、プログラム実行装置300の実行対象となるオブジェクトプログラムの取得経路も図2に示したものに限定されることはなく、例えばBluetooth、HomeRF等に定められているような方法でオブジェクトプロ

ラムが伝送されることとしてもよい。

(6) 本実施の形態では、ダウンロードするアプリケーションプログラム、即ちオブジェクトプログラムはJavaクラスファイルであることとしたが、これに限定されることはなく、機械語プログラムであることとしてもよい。機械語プログラムの場合にはプログラム解釈実行部301はCPUであることとし、使用機能監視部302はいわゆるプログラムカウンタに相当するレジスタが変化する毎に各レジスタ及びメモリを参照して次に実行される命令を監視することとしてもよい。

(7) 本実施の形態で示した図10のステップS306は、実行プログラムの解釈実行を終了するだけであるが、ステップS306はさらに、終了した実行プログラムとこれに付随する実行時使用機能情報とを携帯電話機の記憶装置内から削除することとしてもよい。また、ダウンロードしたオブジェクトプログラムをプログラム実行装置300が実行することによって図8のステップS112でYESの分岐に進んだ場合において、次の処理を追加することとしてもよい。その処理は、実行が完了したオブジェクトプログラムを次回以後は通常のインタプリタ等の実行対象とするための処理であり、例えばそのオブジェクトプログラムのファイル名を安全であるアプリケーションプログラムのリストに登録する処理や、Javaクラスファイルのアトリビュート情報に安全である旨の情報を記録する処理等が考えられる。なお、オブジェクトプログラムが通常のインタプリタ等の実行対象となるということの意味は、使用機能監視等の不正な機能の実行を抑止するための処理を行うことなく実行されるということである。従って、例えば安全であるアプリケーションプログラムのリストに登録されているオブジェクトプログラム、安全である旨の情報が付加されたオブジェクトプログラム等の安全性が保証されたプログラムについては、プログラム実行装置300が不正な機能の実行を抑止することなく従来のインタプリタと同様の機能のみを用いてそのプログラムを実行することとしてもよい。

(8) 本実施の形態で示したプログラム生成装置200は、オブジェクトプログラムを生成した後に、そのオブジェクトプログラムが使用する機能の機能IDを検索して実行時使用機能情報を生成することとしたが、C言語やJava言語等で記述されたソースプログラムをオブジェクトプログラムに翻訳する過程において、そのオブジェクトプログラムを使用することになる機能を把握して実行時使用機能情報を生成するものであってもよい。

【0063】また、プログラム生成装置200は、オブジェクトプログラムに含める実行時使用機能情報を、配信経路における改竄から保護するために暗号化することとしてもよい。この場合にはプログラム実行装置300側では実行時使用機能情報を復号して参照するようにする必要がある。

(9) 本実施の形態では、個人情報領域には、人物名、電話番号、メールアドレスその他の個人情報が含まれることとして、ダウンロードしたオブジェクトプログラムによる個人情報領域へのデータ書込又は個人情報領域からのデータ読出の機能の使用を禁止することとし、またユーザは使用禁止テーブルの更新によりこれらの機能の使用を禁止から許可に変更することができることとした。このように個人情報をひとまとめに管理するのではなく、個人情報を複数の種別に区分して種別毎に管理することとしてもよい。即ち、個人情報領域を第1種個人情報領域、第2種個人情報領域、第3種個人情報領域等と区分して、この区分された領域毎に、ダウンロードしたオブジェクトプログラムによるデータ書込や読出の禁止又は許可の制御を行うこととしてもよい。

(10) 本実施の形態において実行プログラムの解釈実行に関して用いた「停止」という用語は、図8のステップS101、S102に示した処理等を実行プログラムの起動前に行う場合には解釈実行の「抑止」を意味する。なお、実行プログラムが複数のモジュールから構成される場合においてプログラム実行装置300が各モジュールを必要時に動的にメモリにロードして実行することとしてもよく、この場合にはロード直後にステップS101～S103の処理を行うこととしてもよいので、必ずしも実行プログラムの起動前に解釈実行を抑止するとは限らず、実行プログラムの実行中に解釈実行を停止するケースも起り得る。

(11) 本実施の形態において図11に示した画面には、実行プログラムがどの機能を使用することになるために停止されたか等、停止を解除させるべきか否かのユーザによる判断に有用な情報を付加することとしてもよい。

(12) 本実施の形態におけるプログラム実行装置300の処理手順(図8～図10に示した手順等)を、プログラム実行機能を有する家電機器、携帯情報端末等に行わせるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。このような記録媒体には、ICカード、光ディスク、フレキシブルディスク、ROM等がある。流通、頒布されたコンピュータプログラムは、家電機器、携帯情報端末等にインストール等されることにより利用に供され、家電機器、携帯情報端末等は、前記コンピュータプログラムを実行して本実施の形態で示したようなプログラム実行装置を実現する。

【0064】

【発明の効果】以上の説明から明らかなように、本発明に係るプログラム実行制御装置は、機器に搭載されており、前記機器の特定の資源を利用する機能群のうち自らが使用する機能を示す使用機能情報が付加されたプログラムを取得して、実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取

得したプログラムを実行する実行手段と、前記使用機能情報に基づく判断を行い、判断結果がプログラムの実行が不適当であることを表す所定の場合に、前記実行手段によるプログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0065】これにより、予めプログラムに、そのプログラムが使用する機能を示す使用機能情報が付加されているので、この使用機能情報を利用することにより比較的簡易な方法でセキュリティを確保することが可能になる。即ち、使用機能情報と実際のプログラムの動作とを比べることによりそのプログラムが改竄されていることを検出することや、使用機能情報を参照することにより、使用を禁止すべき機能をそのプログラムが使用するかどうかを検出することが簡易な構成で実現できるようになる。

【0066】また、前記プログラムは複数の命令を含み、前記実行手段は前記プログラム中の命令を実行するものであり、前記停止手段は、実行中のプログラムにおける次に実行対象となる命令を監視し、前記命令が前記機能群のうち前記使用機能情報において使用する機能として示されていない機能を使用する命令であった場合に前記実行手段による前記プログラムの実行を停止させることとしてもよい。

【0067】これにより、ダウンロードしたプログラムに付加されておりそのプログラムが使用する機能を示す使用機能情報と、実際の動作時にそのプログラムが使用しようとする機能を監視した結果とを比較することになるので、使用機能情報とプログラムとの相違を検出することができる。従ってプログラム生成時においては使用機能情報とプログラムとは整合するものであることを前提とすると、プログラムが通信路において不正に改竄されていることが簡単に検出できることになり、不正に改竄されたプログラムの実行による被害を防止することができるようになる。

【0068】また、前記使用機能情報は暗号化されており、前記停止手段は前記使用機能情報を復号して参照することとしてもよい。これにより、使用機能情報が暗号化されているために通信経路においてプログラムと使用機能情報との両方を不正に書き換えることが困難になり、その結果、プログラムと使用機能情報との不整合を調べることによりプログラムの改竄は容易に検出可能となる。

【0069】また、前記プログラム実行制御装置は、使用を禁止する機能を示す禁止機能情報を記憶する禁止機能記憶手段を備え、前記停止手段は、前記禁止機能情報に示されている使用を禁止する機能が前記使用機能情報に使用する機能として示されている場合には前記実行手段によるプログラムの実行を停止させることとしてもよい。

【0070】これにより、危険等の理由から予め使用

禁止するものと定めている機能を、使用することが示されているプログラムの実行を停止するので、使用機能情報と禁止機能情報の比較だけの簡易な方法により安全性が確保できる。なお、ここでいう停止にはプログラム実行そのものを行わない抑止も含まれる。また、前記禁止機能情報が示す使用を禁止する機能には、少なくとも無線通信の機能が含まれることとしてもよい。

【0071】これにより、機密情報の流出の可能性がある、また通信料金が必要となる場合もあり得る等の理由から、ダウンロードしたプログラムに自由に使用させるのは問題がある無線通信機能を使用するプログラムを停止することができる。また、前記禁止機能情報が示す使用を禁止する機能には、少なくとも出力デバイスからのデータ出力の機能が含まれることとしてもよい。

【0072】これにより、ダウンロードしたプログラムがディスプレイにパスワード等の秘密の情報を表示する等の出力動作を行うことを防止することができる。また、前記禁止機能情報が示す使用を禁止する機能には、少なくとも入力デバイスからのデータ取得の機能が含まれることとしてもよい。これにより、ダウンロードしたプログラムがマイクを通じてデータを取得して盗聴を行う等のデータ取得動作を行うことを防止することができる。

【0073】また、前記プログラム実行制御装置はさらに、ユーザの操作を受け付けて前記操作に応じて前記禁止機能情報を更新する禁止機能変更手段を備えることとしてもよい。これにより、危険等の理由から予め使用を禁止するものと定めている機能についてもユーザによっては危険と考えない場合もあり得ることに対応し、ダウンロードしたプログラムに使用させたくない機能をユーザが自由に設定できるようになる。

【0074】また、本発明に係るプログラム実行制御装置は、個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域からのデータ読出を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0075】これにより、携帯情報端末に通常記憶されておりプライバシーに関わる情報である個人情報をダウンロードしたプログラムが読み出すことを防ぐことができるので、個人情報の流出を阻止できるようになる。また、本発明に係るプログラム実行制御装置は、個人情報領域を有するメモリを備える携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実

行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記個人情報領域へのデータ書込を行う命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0076】これにより、携帯情報端末に通常記憶されておりプライバシーに関わる情報である個人情報をダウンロードしたプログラムが書き換えることを防ぐことができるようになる。また、本発明に係るプログラム実行制御装置は、携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末の外部と通信する機能処理ルーチンと呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0077】ここで、機能処理ルーチンとはアプリケーションプログラムの実行環境に存在し、そのアプリケーションプログラムから呼び出され何らかの処理を行ういわゆるサブルーチンであり、例えば `invoke virtual` 等のライブラリ呼出命令により呼び出されるライブラリプログラムである。これにより、ダウンロードしたプログラムが携帯情報端末の外部と通信する機能を使用することを防ぐことができるようになる。これは例えばユーザの意図と関係なく通信料金が必要となる事態が生じるのを防ぐ等の意味を持つ点で有用である。

【0078】また、前記機能処理ルーチンは前記携帯情報端末の外部へのデータ送信を行う機能処理ルーチンであることとしてもよい。これにより、携帯情報端末からの機密情報の流出を防ぐことができるようになる。また、本発明に係るプログラム実行制御装置は、携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であって、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える出力デバイスからのデータ出力を行う機能処理ルーチンと呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0079】これにより、ダウンロードしたプログラムが携帯情報端末のディスプレイにパスワード等の秘密の情報を表示する等の出力動作を行うことを防止することができる。また、本発明に係るプログラム実行制御装置は、携帯情報端末に搭載され、複数の命令からなるプログラムを取得して実行するプログラム実行制御装置であ

って、通信路からプログラムを取得する取得手段と、取得したプログラムを実行する実行手段と、実行中のプログラムが次に実行しようとする命令を監視し、前記命令が前記携帯情報端末が備える機能処理ルーチンであって前記携帯情報端末が備える入力デバイスからのデータ取得を行う機能処理ルーチンと呼び出す命令である場合に前記実行手段による前記プログラムの実行を停止させる停止手段とを備えることを特徴とする。

【0080】これにより、ダウンロードしたプログラムが携帯情報端末に備えられたマイクを通じてデータを取得して盗聴を行う等のデータ取得動作を行うことを防止することができる。また、前記プログラム実行制御装置はさらに、前記停止手段によって前記プログラムの実行が停止した場合に、停止した旨をユーザに通知する通知手段を備えることとしてもよい。

【0081】これにより、ユーザはダウンロードしたプログラムの実行が停止されたことを知ることができるようになる。また、前記プログラム実行制御装置はさらに、前記停止手段によって前記プログラムの実行が停止した場合に、ユーザによる入力を受け付けて前記入力に応じて停止を解除する停止解除手段を備えることとしてもよい。

【0082】これにより、ユーザはプログラムの実行が停止された場合にその停止を自己の判断によって解除することができるようになる。

#### 【図面の簡単な説明】

【図1】本発明の実施の形態に係るプログラム実行装置300等の構成図である。

【図2】プログラム実行装置300を備える携帯電話機とダウンロード対象のオブジェクトプログラムとの関係を示す図である。

【図3】機能IDテーブルのデータ構造及び内容例を示す図である。

【図4】オブジェクトプログラムに付加される実行時使用機能情報のデータ構造及び内容例を示す図である。

【図5】使用禁止テーブル304のデータ構造及び内容例を示す図である。

【図6】メモリ内の領域の分類を示した図である。

【図7】個人情報の内容の具体例を示す図である。

【図8】プログラム実行装置300がダウンロードしたオブジェクトプログラムを解釈実行する際における処理手順を示すフローチャートである。

【図9】使用機能監視部302による監視処理を示すフローチャートである。

【図10】解釈実行停止処理を示すフローチャートである。

【図11】ユーザ通達部307の制御によりディスプレイに表示される画面の例を示す図である。

【図12】ユーザ禁止指定入力部309が携帯電話機のディスプレイに表示するよう制御する使用禁止機能選択

10

20

30

40

50

23

24

画面を示す図である。

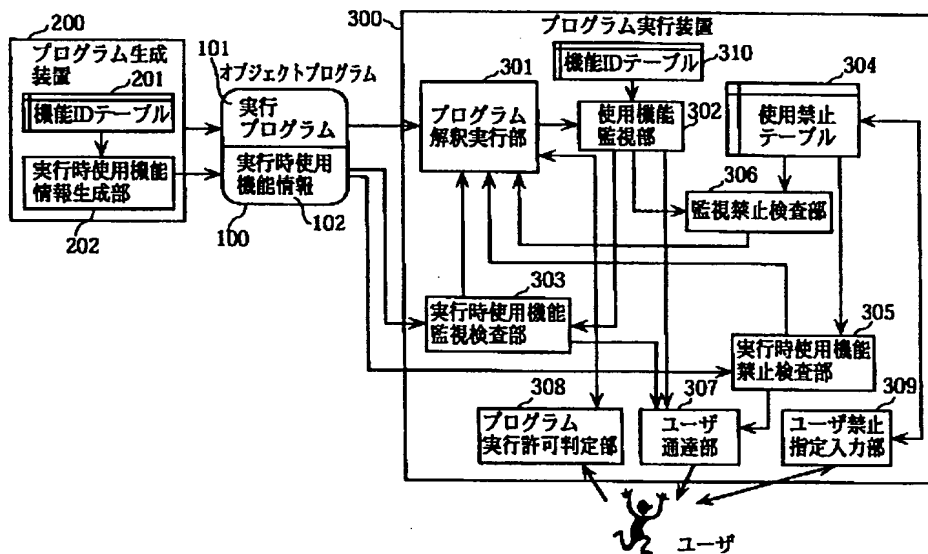
【図 13】メモリ内に個人情報であるデータと個人情報以外であるデータがフラグによって識別可能となるように格納されている例を示す図である。

【符号の説明】

100 オブジェクトプログラム  
101 実行プログラム  
102 実行時使用機能情報  
200 プログラム生成装置  
201 機能IDテーブル  
202 実行時使用機能情報生成部  
300 プログラム解釈実行装置

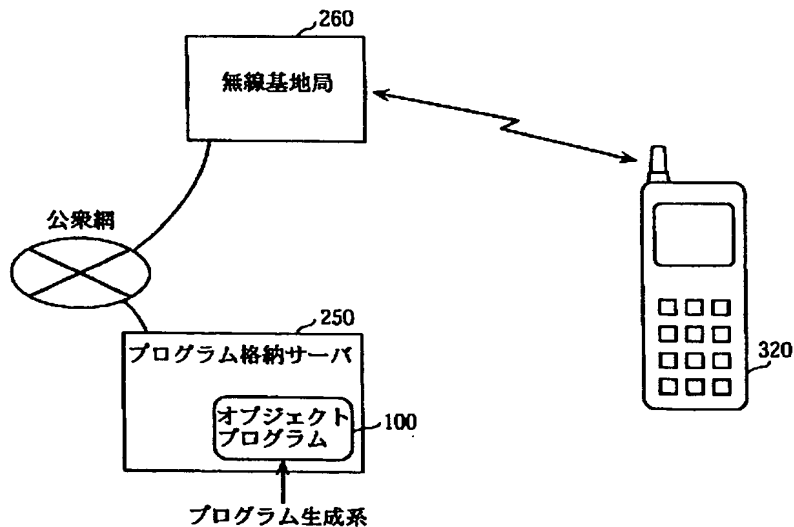
300 プログラム実行装置  
301 プログラム解釈実行部  
302 使用機能監視部  
303 実行時使用機能監視検査部  
304 使用禁止テーブル  
305 実行時使用機能禁止検査部  
306 監視禁止検査部  
307 ユーザ通達部  
308 プログラム実行許可判定部  
10 309 ユーザ禁止指定入力部  
310 機能IDテーブル

【図 1】



【図 2】

【図 4】



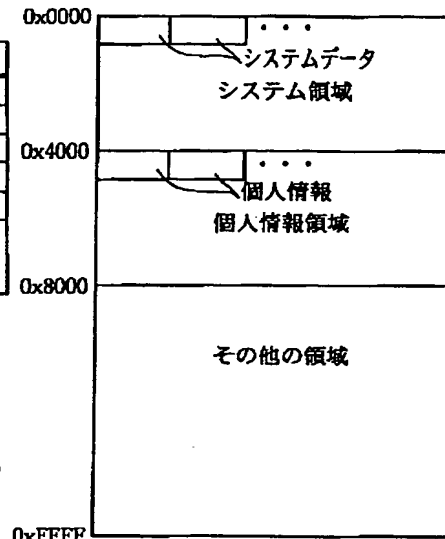
実行時使用機能情報

機能ID	フラグ
0x0001	0x00
0x0002	0x01
0x0003	0x00
0x0004	0x01
0x0005	0x00
⋮	⋮

【図 3】

機能ID	ライブラリ番号
0x0001 (無線I/Fへのデータ出力)	6
0x0002 (ディスプレイへのデータ出力)	7
0x0003 (音声出力回路へのデータ出力)	8
0x0004 (無線I/Fからのデータ入力)	32
0x0005 (ボタンからのデータ入力)	33
⋮	⋮

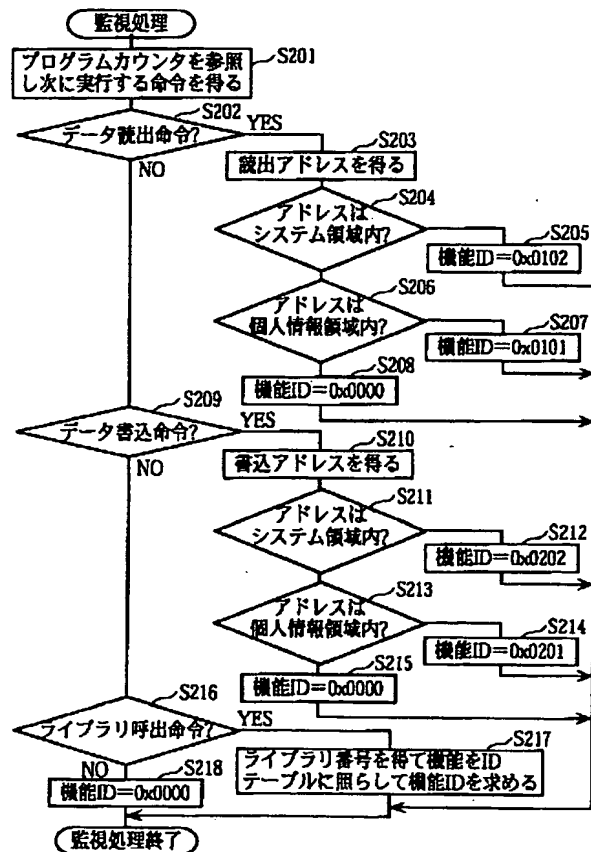
【図 6】



【図 5】

機能ID	フラグ
0x0001 (無線I/Fへのデータ出力)	0x00
0x0002 (ディスプレイへのデータ出力)	0x01
0x0003 (音声出力回路へのデータ出力)	0x01
0x0004 (無線I/Fからのデータ入力)	0x00
0x0005 (ボタンからのデータ入力)	0x01
⋮	⋮
0x0101 (個人情報領域からのデータ読出)	0x00
0x0102 (システム領域からのデータ読出)	0x00
0x0201 (個人情報領域へのデータ書込)	0x00
0x0202 (システム領域へのデータ書込)	0x00
⋮	⋮

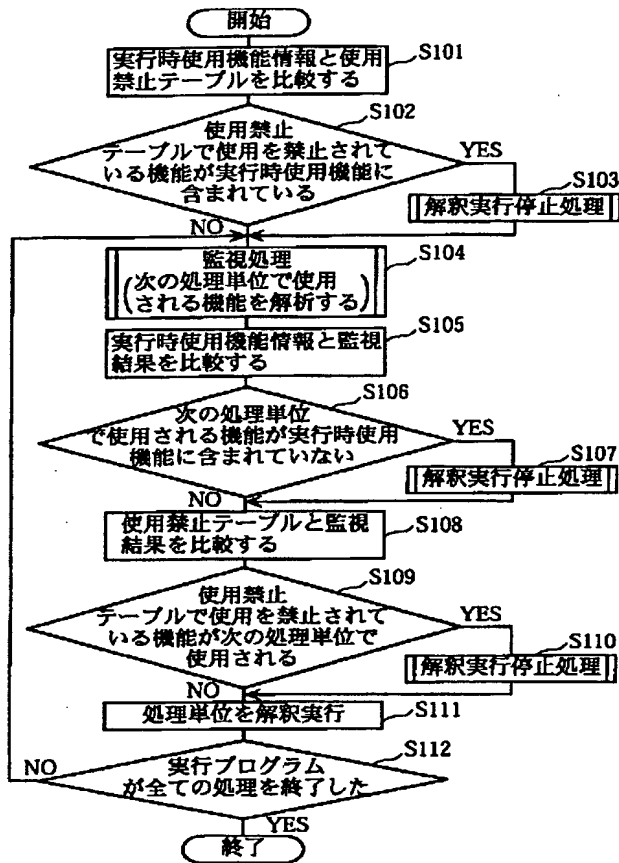
【図 9】



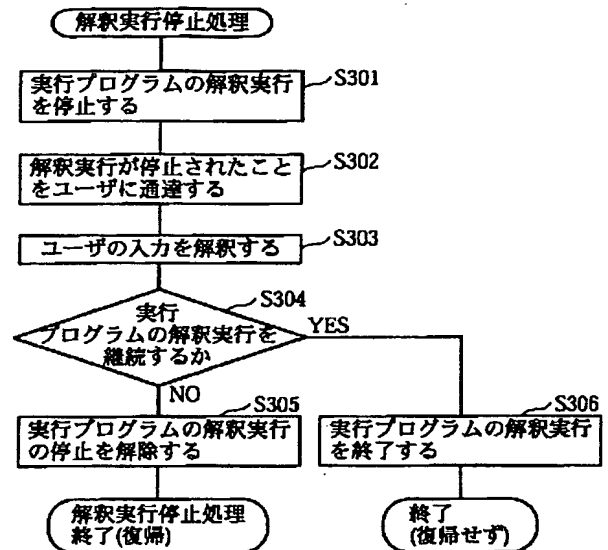
【図 7】

- ・人物名
- ・電話番号
- ・住所
- ・メールアドレス
- ・伝言メモ
- ・機器の設定、例えば、携帯電話を例にすると、
  - －着信音量
  - －通話音量
  - －着信通知の設定(着信音か、バイブレーションか、あるいは別の手段か)
  - －着信時に演奏されるメロディ
  - －アラーム使用時刻
  - －課金状況
  - －機器の使用時間
  - －留守番電話にしているか否か
  - －FAXを受けられるか否か

【図 8】



【図 10】



【図 11】

Notice :

プログラム"maze.cj"の  
実行が停止されました

■実行を継続しますか?

"1" — Yes

"0" — No

2000/03/29 Wed 18:01:53

【図 12】

■ 使用禁止機能選択画面 ■

個人情報領域からのデータ読出

個人情報領域へのデータ書込

無線送信機能

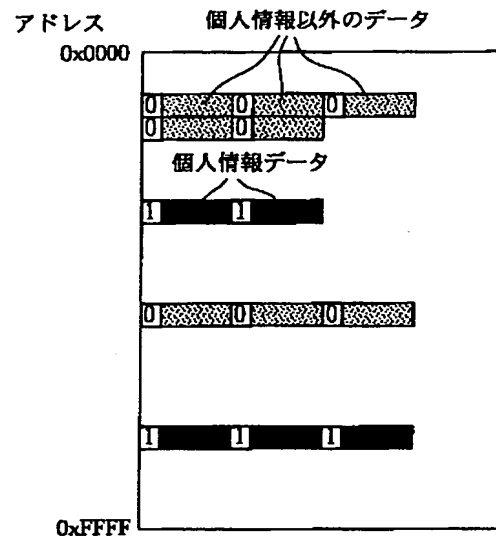
"1" — 使用を許可

"0" — 使用を禁止

2000/03/29 Wed 18:20:24



【図 13】



---

フロントページの続き

(72)発明者 富永 宣輝  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 春名 修介  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

Fターム(参考) 5B017 AA08 BB06 CA15  
5B076 BB06 FA00 FB02